INFORMATION PAPER

NETC-EST-IA
31 August 2005

SUBJECT: Army CAC Cryptographic Logon

1. Purpose. Provide information on the Army CAC Cryptographic Logon Project.

2. Facts.

a. The Army Common Access Card (CAC) Cryptographic Logon (CCL) project will enable smart card certificate-based logon to unclassified computer networks. CAC holders will logon to the network using their CAC and associated Personal Identification Number (PIN) instead of a username and password. Logging on using CCL increases security and provides users a more efficient way to authenticate to network resources. CCL increases security by providing 2-factor authentication allowing users to be authenticated with something they know [e.g., a Personal Identification Number (PIN)] and something they have (CAC with DoD PKI certificates). Efficiency is gained by using an easy to remember 6-8 digit PIN instead of a complex, ever-changing password.

b. The following infrastructure requirements and/or services are needed prior to providing this capability:

(1) Active Directory implementation completed or in-progress.

(2) Changes to the Army's enterprise-wide Active Directory network.

(a) User Logon Name: A change to the user's Active Directory account must contain their unique 10-digit Electronic Data Interchange – Person Identifier (EDI-PI) and "@mil" suffix (EDI-PI@mil).

(b) DoD root and intermediate Certificate Authority (CA) certificates in both the Authority Information Access (AIA) and the NTAuth stores.

(3) Machine certificate issued to the domain controller with both "Client Authentication (1.3.6.1.5.5.7.3.2)" and "Server Authentication (1.3.6.1.5.5.7.3.1)" properties in the "Enhanced Key Usage" field.

(4) Certificate validation software implemented on domain controllers.

(5) Army Automated Name Provisioning Tool that automates registration and update of CAC user's EDI-PI information into Active Directory.

(6) CACs must be configured with three PKI certificates (identity, email signature and email encryption).

(7) User workstations have Windows 2000 or XP operating systems, functioning smart card readers, and middleware (ActivCard 3.0 or greater or NetSign 4.2 or greater).

c. Activities are well underway to address the requirements/services identified above. Active Directory has been fielded at most Army installations and a certificate validation solution has been selected and deployment is expected during the first quarter, FY06. Configuration change proposals have been submitted to the Army Enterprise Infrastructure Change Control Board to obtain enterprise-wide approval for the required Active Directory modifications. The Army Automated Name Provisioning Tool has been developed and scheduled to undergo an operational assessment the first week of Oct 05. Lastly, user workstation smart card readers and middleware have already been widely implemented throughout the Army.

d. A CCL implementation guide will be released by 14 Nov 05. It will provide step-by-step technical instructions to enable CCL services. Additionally, it will provide standardized, repeatable, well-written guidance, templates (event timelines, lessons learned, communication plan, etc.) and best practices for programmatic activities. The Army Automated Name Provisioning Tool will be provided to each installation and provide two services. The first service is a client web-form allowing CAC users to self-register their EDI-PI information. The second service allows system administration personnel an automated process to provision those accounts. The tool will automatically notify users via an email once their Active Directory account has been provisioned. Training on all activities required to implement CCL will be provided to local installations. It is envisioned the training will be provided via web cast.

e. A phased approach will be used to introduce the CCL capability. The initial phase was completed during a certificate validation operational assessment conducted at Fort Dix New Jersey in Jan/Feb 05. The CCL capability was successfully implemented during the OA and is still in use. The second phase will consist of conducting initial fielding at one location during the first quarter, FY06. The third phase objective is to deploy the CCL capability Army-wide beginning in second quarter, FY06. Planning and coordination with key stakeholders for this phase has just begun. The goal is to coordinate implementation efforts with all organizations affected by CCL and give them an opportunity to provide input on how CCL should be implemented and identify any possible issues from its implementation. Follow-on phases may be required to address unique issues that arise from initial CCL implementation and work towards a goal of mandating CCL to access Army networks.

Mr. Kevin Watkins/703-602-7511
Approved by_____